KNOW GREATER VALUE™

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Roundup – April 2018

By Thomas J. DeMayo, Principal, Cyber Risk Management

It's been one year since *Cyber Roundup* was launched. To quote us in our first online newsletter, we said our monthly mission was to report: ***happenings that are not only important to be aware of but may have implications for any organization operating in today's digital age.*** The mission continues.

Unfortunately, many of the bulleted items presented each month are not exactly "uplifting" but we are obliged to report them so our readers stay informed and on guard. Where appropriate, we also add our professional perspective. We want to remind our readers that PKF O'Connor Davies, LLP has the staff and the expertise to be of assistance to you as you arm yourself and your business against cyber predators.

Key Cyber Events

The following is a rundown of what happened during the month of March 2018. We welcome your comments, insights and questions.

- **Orbitz, an Expedia subsidiary, announced that the credit card payment details of approximately 880,000 users may have been compromised.** The cyber incident was identified on March 1, 2018 and affected a legacy travel booking platform. The breach may have also affected select business partners. The breach is currently limited to purchases made on the Orbitz platform between January 1, 2016 and June 22, 2016, and between June 1,2016 and December 22, 2017 for select partners. Orbitz has noted that passport information was not part of the breached data.

- **The city of Atlanta was the most recent municipality victimized by a ransomware attack.** The attack caused major disruptions to five of the city's 13 departments. The strain of ransomware that affected this city is dubbed SamSam. SamSam, unlike most ransomware variants, does not rely on phishing or users to spread, but instead relies on weakness in publicly available systems, ranging from weak credentials to unpatched vulnerabilities. It is unfortunate, but most municipalities do not allocate funds to help develop a strong cyber program to have a fighting chance against cyber attacks. Until municipalities start to allocate funds to these areas, cyber incidents will continue to occur.

- **Facebook became involved in a major scandal that pertained to the misuse of the personal information of 50 million users (later updated to 87 million).** Cambridge Analytica, a political data firm, used the personal information to understand personality traits and target ads to help influence voter behavior. The source of the original data dates back to 2014, when a company, Global Science Research, created an app that paid users to a take a psychological test. The app is what mined the Facebook data. It is reported that only 270,000 users who participated in the survey actually consented to have their data harvested; however, the consent was based on the data being used for academic purposes. The harvested information was subsequently sold to Cambridge Analytica. The investigation is ongoing.

- **Applebee's restaurants suffered a breach of their point of sale systems resulting in the theft of payment card information.** The breach was discovered February 13, 2018 and is believed to have affected transactions that occurred between December 6, 2017 and January 2, 2018. The breach affected more than 160 locations across the U.S.

- **GitHub, a popular software development platform, experienced the worst distributed denial of service (DDOS) attack in history.** A DDOS attack is when multiple distributed hosts are used to flood a service with a massive amount of traffic that it becomes overloaded and can

no longer process legitimate requests. At its peak, the site was hit with 1.35 terabits of data per second. Fortunately, GitHub subscribed to a DDOS mitigation service, Akamai Prolexic, that was able to stop the attack. It is without question that DDOS attacks will become more prevalent and damaging over time as the internet of things continues to expand.

- **The U.S. imposed new sanctions against Russia for launching cyberattacks on the U.S. energy grid.** The Department of Homeland Security (DHS) issued an alert on what it categorized as a multi-stage campaign against select government entities and critical infrastructure sectors. The DHS reported that the Russian hackers targeted smaller commercial network facilities that were not as secure to gain access to the energy sector networks. The attack of less secure third parties is a common tactic often used by cyber criminals to gain access to larger entities that are the point of interest. Third parties need to be assessed to ensure that their security controls are effective and that the risk they pose is properly understood and managed.

- **A Saudi petrochemical plant was targeted by hackers in an attempt to trigger an explosion.** In what is believed to be a state sponsored attack, the hackers' code failed and, instead of triggering the explosion as designed, it resulted in the shutdown of the systems. The attack is believed to be politically motivated. A statement has not been made as to who is believed to be behind the hack.

- **St. Peter's Surgery & Endoscopy Center reported that a breach occurred impacting approximately 135,000 patients.** This healthcare data breach is the second largest in 2018 and the fifth largest on record in New York State. The breach occurred and was discovered on January 8, 2018. Although the center rapidly detected the malware, it could not with certainty rule out unauthorized data access or theft.

Contact Us

Thomas J. DeMayo, Principal, Cyber Risk Management
CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE

PKF O'Connor Davies, LLP
665 Fifth Avenue, New York, NY, 10022
212.867.8000 or 646.449.6353 (direct)
tdemayo@pkfod.com

www.pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, nine offices in New York, New Jersey, Connecticut and Maryland, and more than 700 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 29th on *Accounting Today*'s 2018 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today.* In 2018, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.